MB 04-65

real™

February 27, 2004

Federal Communications Commission
Office of the Secretary
Attn: Broadcast Flag Certifications
9300 East Hampton Drive
Capitol Heights, MD 20743

Re: DA 04-145

TO WHOM IT MAY CONCERN:

Attached you will find RealNetworks submission for technologies to be considered as an Approved Recording Method and an Authorized Digital Output Protection Technology, submitted pursuant to Public Notice DA 04-145.

RealNetworks submits two technologies for consideration. We submit Helix DRM Trusted Recorder for consideration as an Approved Recording Method. We also submit Helix Device DRM for consideration as an Authorized Digital Output Protection Technology.

RealNetworks is pleased to submit these technologies for consideration. Our digital rights management product, Helix DRM, is widely used by content and service providers to securely deliver top tier movies and video over the Internet to consumers today. We look forward to extending this product into the digital television space through its certification as technology capable of supporting the Broadcast Flag.

Please do not hesitate to contact us should you have any questions.

Sincerely,

Sherman Griffin
Director, Marketing
RealNetworks, Inc.

P O Box 91123 • Seattle • WA • 98111-9223 (PH) 206.674.2700 (FX) 206.674.2699 www.real.com

Networks

MB Docket 04 - _____

Broadcast Flag Certification Response
to the
Federal Communications Commission

Response to Public Notice DA 04-125 on January 23, 2004

February 27, 2004

RealNetworks, Inc.
2601 Elliott Avenue
Seattle, WA 98109

This document is in response to FCC Public Notice DA 04-145, announcement of the initial certification filing window for proponents of digital output protection technologies and recording methods. It submits RealNetworks Helix DRM to the FCC to be considered as a) an Approved Recording Method, and b) an Authorized Digital Output Protection Technology.

All comments, questions, or follow-up communications should be addressed to:

RealNetworks, Inc.

Attn: Surya Mantha

2601 Elliott Avenue

Seattle, WA 98121

206-674-2246

smantha@real.com

http://www.realnetworks.com

Table of Contents

1 Executive Summary

RealNetworks is the leading provider of IP network delivered audio and video services and the creator of technology that enables digital media creation, distribution, security and consumption. Committed to standards since its founding, the company continues to compete with a universal media and technology strategy that differentiates it favorably from other companies in the marketplace. RealNetworks digital rights management product, Helix DRM, is an ideal universal digital content protection technology that can be used to securely package, transfer, and playback high value content marked with the Broadcast Flag.

The move to digital television combined with the advent of continuing improvements in Internet technology, including widespread broadband availability, consumer home networks, and new consumer electronics devices, introduces risks of piracy and widespread distribution of unauthorized, stolen content. Content providers, operators, and device manufacturers are faced with the challenge of leveraging this technology explosion to deliver high-value media to consumers, while simultaneously ensuring the protection of this content.

Digital rights management provides an innovative solution for content providers, operators, device manufacturers, and consumers through the application of cryptographic technology and computer security. It offers high-quality media to consumers while protecting media ownership rights.

RealNetworks believes that digital rights management technology is essential to creating a digital media marketplace for media. With Helix DRM, RealNetworks has introduced the leading digital rights management platform that enables the association of business rules with all valuable media content. By leveraging the end-to-end, robust rights management technologies of Helix DRM and using it in conjunction with the ATSC Broadcast Flag, rights owners can now develop successful business models to make their valuable assets available to large audiences over the Internet.

Helix DRM is built on RealNetworks commercially shipping and widely used Helix platform. The Helix platform is a set of technologies licensable on RAND-based licensing terms and is widely licensed by the consumer electronics industry. In addition, the Helix platform is operating system independent, designed to work on the many operating systems used by the consumer electronics industry. Implementations are available or underway on a wide range of operating systems including Linux, WinCE, iTron, PSOS, VXWorks, Palm, Symbian, SmartPhone, MAC, and Windows.

In this submission, RealNetworks proposes its Helix DRM Trusted Recorder technology as an Approved Recording Method. Leveraging the widely used and supported Helix DRM, the Trusted Recorder technology creates a complete end-to-end DRM solution on Covered Devices that enables the protection, playback, and transfer of Broadcast Flag enabled content. In essence, with this solution Broadcast Flag enabled content is ingested into the Trusted Recorder, where the Trusted Recorder then recognizes the state of the Broadcast Flag, encrypts the content, applies the correct key associated with that particular state of the Broadcast Flag, and delivers the content for playback. Other devices protected by an Authorized Digital Output Protection Technology will be

able to receive and playback the secure Broadcast Flag enabled content pursuant to the previously identified state.

RealNetworks also submits its Helix Device DRM protocol as an Authorized Digital Output Protection Technology. This protocol enables the secure receipt and playback of content encrypted using Helix DRM Trusted Recorder. Helix Device DRM is a commercially shipping technology, available on devices today, supporting content from all major record labels.

Helix DRM was designed from the beginning to be a complete end-to-end DRM system that spans beyond just the PC, Internet, and Broadcast spaces. As the consumer demand for secure and ubiquitous content grows, this demand will occur on a variety of platforms—mobile phones, automobiles to name a few. Present in all of these platforms are standards-based initiatives to ensure a universal marketplace. RealNetworks' approach to the market is to enable the support of standards so that the full digital media marketplace can be realized. To this end, Helix DRM has been designed to work with standards based initiatives and potential Authorized Digital Output Protection Technology techniques such as DTCP / IP and CPRM. As proof of our commitment to secure digital media standards we recently announced support for OMA, the Open Mobile Alliance in the mobile handset market; Helix DRM transcrypts to OMA compatible devices, thereby enabling an end-to-end secure content solution in the mobile market. While we will support additional secure media standards, for time to market reasons and interoperability with current devices in the market, we have shipped Helix Device DRM commercially and hereby submit it for consideration as an Authorized Digital Output Protection Technology.

2 A General Description of How the Digital Output Protection Technology Or Recording Method Works, Including Its Scope of Redistribution

2.1 RealNetworks Solution to Media Rights Management: Helix DRM

Helix DRM has been designed to meet the following goals:

- Satisfies the needs of content owners and corresponding rights holder
- Enables a number of flexible business models including but not limited to subscription, video on demand (VOD), and other innovative media commerce business models
- Protects the content owner from piracy attempts or unauthorized access
- Provides value to consumers by offering content that would otherwise be unavailable without the use of rights management technology
- Interoperates with Standards based requirements including the ATSC Flag, DTCP / IP, OMA, CPRM, *and others*
- Is codec independent and allows the support of any codec
- Is interoperable on any operating system or platform
- Offers secured digital media to the widest audience possible by making it available on desktops, set-top boxes, consumer electronics devices, home networks, or portable device deployments
- Transparently delivers secured media to consumers and seamlessly enforces rights during playback, so users receive and play secured media in the same manner as other media files

2.2 Understanding Helix DRM

The following is designed as an overview of the Helix DRM product. Helix DRM provides three components to protect, deliver, and enforce rights for media:

- Helix DRM Packager— The Helix DRM Packager uses strong encryption algorithms and secure container technology to prevent unauthorized use of content and to prepare content for distribution via streaming, download or other delivery methods. The packaged media content and the associated business rules for unlocking and using that content are stored separately, so that multiple sets of business rules can be applied to a single file over time. The Helix DRM Packager can support a wide range of media formats and can deliver secure live content.
- Helix DRM License Server — The Helix DRM License Server is a scalable, flexible server that allows any entity including retailers, music and movie services, content providers, broadcasters, and enterprises to manage, authorize, and report content transactions. The Helix DRM License Server verifies content licensing requests, issues content licenses to trusted, authenticated Helix DRM end-user clients and provides auditing information to facilitate royalty payments. The content owner, in the event of a security Player breach, can also revoke licenses.
- Helix DRM Client — The Helix DRM client enables download and streaming playback of secure formats in a trusted, tamper-resistant environment based on the usage rules specified by the content owners. The Helix DRM Client can be supported on any operating system, including the many used by the consumer electronics manufacturers. Current operating systems supported or with projects underway include Linux, WinCE, iTron, PSOS, VXWorks, Palm, Symbian, SmartPhone, MAC, Windows.

These components interact with existing content delivery mechanisms, a retail Web server and a back-end database. These three components consist of:

- Existing delivery mechanisms to deliver secured content. Secure files can be delivered on virtually any delivery mechanism: broadcast networks, traditional File Transfer Protocol (FTP) downloads, peer-to-peer networks, multicasting or traditional medium like CDs or DVDs.
- Back-end Database. A content database, which stores identifying information for each content file: the secured content key and a globally unique identifier. It inputs this data from Helix DRM Packager and makes it available to the retail Web server during content licensing.
- The retail Web server--an existing front-end Web site through which consumers request licenses to secured content. The retail Web server sends these requests to Helix DRM License Server and returns the licenses generated by Helix DRM License Server to the consumer

Integral to the solution is the Helix DRM System that includes a Helix DRM Packager, a Helix DRM License Server as well as a trusted client environment for RealPlayer 10 and other Helix DNA based media players. Helix DRM supports multiple media formats including leading Internet formats like RealAudio, RealVideo and MP3 as well as other standards based formats including MPEG-4, AAC, H263. In addition, RealNetworks expects to support other standards such as H.264 as they become published and finalized.

Typically, a DRM system supports a variety of rights. RealNetworks' Helix DRM supports several types and variations, including:

Playback for a limited time period	• From first play • From download
Playback for a specific number of times	• Unrestricted but capture counter • Restricted to a count limit • Configurable threshold time to constitute a play and increment counter
A specific number and type of copies	• Number of times transferred to Red Book Audio (i.e. CDROM) • Number of times transferred to unsecured file (e.g. MP3) (Note, this is not likely to be granted)
A specific number of transfers to a portable device	• Number of times transferred to a secure device (e.g. SDMI compliant) • Number of times transferred to Helix DRM compatible devices • Number of times transferred to OMG and SD memory cards

Additionally, Helix DRM is based on a flexible rights expression language that accommodates flexible future sets of rights including, for example, transfer to DTCP, CPRM, OMA, and other standard or proprietary link and storage protection mechanisms.

RealNetworks has fully examined 5C and other standards-based technologies and is confident of our system's ability to securely export to them.

An example of a typical user experience – both from the consumer and system perspectives -- illustrates some of the Helix DRM functionality and the role of each of the components described above.

First, a consumer acquires a DRM-encrypted file (or "packaged file") via any means of electronic or physical distribution. This file has been rendered inert by the Helix DRM packager and can therefore be safely distributed on any media or over any network. The contents of the file will remain inaccessible until the consumer acquires a license.

To obtain a DRM license, the consumer double-clicks the file, causing the Real Player 10 or a Helix DNA-based media player to load the file. When the Real Player 10 or Helix DNA Player discovers that the file is protected, it consults the Helix DRM Plug-in to determine whether it already has a license for the file. If not, it asks the plug-in to construct a license request that points to a licensing authority – typically a web based storefront or other licensing authority. The address of the licensing authority is specified at the time of packaging and is stored in the encrypted file itself. Any request for a license for that particular file will be directed to that single licensing authority.
The licensing authority determines whether the consumer is entitled to the action requested. If not, the licensing authority could respond with an up-sell or other marketing message. If the consumer is entitled, the licensing authority will request that the Helix DRM License Server construct a license for a specific content Item and a specific client machine. To make a license, the licensing authority or storefront passes

the license server a content key, a few machine-specific details (from the Real Player 10 or Helix DNA client), and the rights the content owner or agent intends to grant the specific consumer in question. The Helix DRM License Server then constructs a license based on the specifications and business rules applied, and then returns the license in encrypted form to the licensing authority or storefront for redelivery to the client. This part of the architecture is designed to allow the license server to remain on a secure network and also to allow licensing authority developers maximum flexibility in developing business applications to manage account level rights.

2.3 Architecture of Helix DRM as an Authorized Digital Content Protection Technology

RealNetworks proposed solution for an Approved Recording Method leverages additions to the Helix DRM client. The technology provides for the Helix DRM client to be modified to operate as a Helix DRM Packager, with a set of individualized encryption keys, one for each possible Broadcast Flag state. The new Helix DRM client ("Trusted Recorder") will be located on the Covered Demodulator Product.

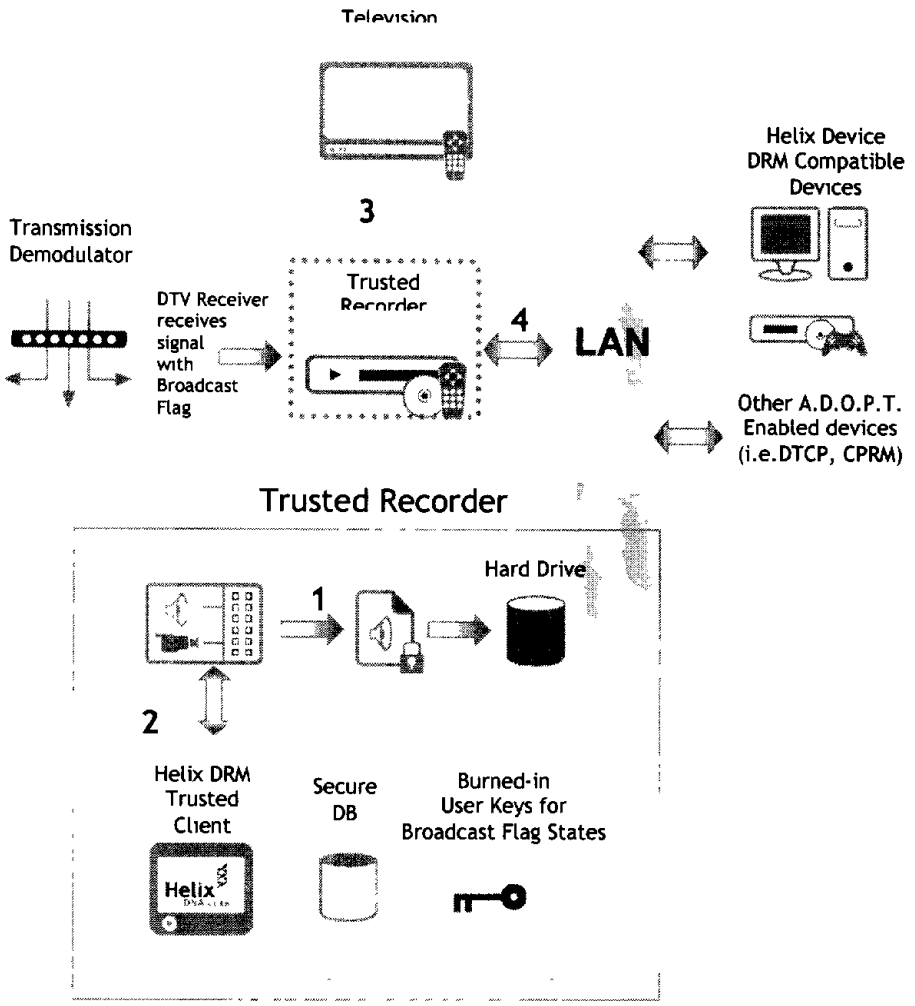
Once the Trusted Recorder receives content, the Trusted Recorder recognizes the state of the Broadcast Flag, and the content is encrypted using the key appropriate to the specified state.

When a device on the same network subsequently requests a Copy of the content, the Trusted Recorder will check the Broadcast Flag state.

- If the state of the Flag is Copy-Never or Copy-No More, the Copy request is denied.
- If the state of the Flag is Copy-Freely, the media is copied to the requesting device. The requesting device then connects to the Trusted Recorder using the Helix Device DRM Protocol to obtain the Copy-Freely key.
- If the state of the Flag is Copy-Once, a new copy of the media file will first be rebound to the Copy-No More key and then transferred. The requesting device then connects to the Trusted Recorder using the Helix Device DRM Protocol to obtain the Copy-No More key.

The benefits of the above solution are as follows:

- Integrity of the Broadcast Flag state is maintained
- Secure content can be delivered to other secure devices in the home, and revenue model integrity can be maintained
- The base security model obeys the Flag states using commercially-deployed rights management software



If content has "Copy Never" or "Copy No More" flag, copy request is denied

If content has "Copy Freely" flag, copy is granted. Trusted Client uses Device DRM Protocol to transfer "Copy Freely" key

If content has "Copy Once" Flag, Trusted Client converts copy to "Copy No More"

1. Local Packager encrypts with random Content Key
2. Local Packager obtains User Key from Helix DRM Trusted Client and encrypts Content Key with appropriate User Key for Broadcast Flag
3. Local client can now consume content
4. Network Authorized Digital Output Protection Technology device requests copy of content from Trusted Recorder

Figure 1. Architecture of Proposed Solution

3 A Detailed Analysis of the Level of Protection the Digital Output Protection Technology or Recording Method Affords Content

3.1 Introduction

This section describes the base-line security architecture for Helix DRM Trusted Client on platforms such as PCs, set-top boxes, or consumer electronics devices, and how Helix DRM Trusted Recorder will act as an Approved Recording Method. It defines the security services requirements, the mechanisms and operations chosen to meet the requirements, and the interfaces between information protection mechanisms in a platform abstracted manner. The method for meeting a requirement may vary from platform to platform. All implementations of the Helix DRM adhere to these standards.

After describing Helix DRM Trusted Recorder, section 3.5 describes how Helix Device DRM acts as an Authorized Digital Output Protection Technology.

3.2 System Description

The Helix DRM enables content providers to protect their content such that only individuals who have been granted the right to play the content will be able to play it back. These rights include the right to play the content back a number of times, for a duration of time, and a full playback right that allows the content to be used indefinitely, by the licensed user. Rights are specified in the form of licenses issued by the content provider or reseller.

The Helix DRM has three components to provide creation, rights assignment, and rights enforcement for multimedia content: the Packager, the License Server, and the Helix DRM Client Update Plug-in to the Helix DNA Client, referred to throughout as the Trusted Client. The Packager application is provided to content providers for them to protect the content. The License Server generates a license to play the content based on a set of rights provided as input. The Trusted Client reads the license and enforces the rights described therein. Sets of cryptographic algorithms are used to provide security and authentication of the rights for this media.

3.2.1 Trusted Client

The Trusted Client is a version of the Helix DNA Client Engine that includes support for authenticating plug-in modules (codecs, renderers, etc.) to establish a trusted playback environment. The trusted environment is known as the "Ecosystem of Confidence" and is established when the Helix DRM Client Update Plug-in validates that the library loading it is trusted by RealNetworks and has not been modified.

3.2.2 Helix DRM Client Update Plug-in

The Client Update Plug-in is the DRM plug-in to the Helix DNA Client media engine. The plug-in stores licenses for content, enforces the rights described in the licenses and does the actual media decryption for rights managed content. The licenses are stored in a secure database file with multiple levels of encryption and digital signatures applied. The media decryption is performed using the content key obtained from the license. Both the Helix DRM Client Update Plug-in and licenses granted to a user are tethered to the device such that neither the code that enforces rights nor the licenses containing the rights can be used on another device.

For broadcast protection, the Helix DRM Client will include a set of default keys and licenses, assigned to the various Flag states. Further, it will include the capability of encrypting content with any of those keys.

3.2.3 Cryptographic Algorithms

The Helix DRM will use strong cryptographic algorithms to implement authentication and secure transfer of sensitive information. All cryptographic algorithms chosen have undergone cryptographic analysis and are deemed to be secure by the cryptographic community. The following algorithms are employed throughout the system. The following sections discuss how the algorithms are used in each component of the system to provide security or authentication.

RSA

An asymmetric algorithm used primarily to create digital signatures, and more rarely for encryption. It is named after its creators: Rivest, Shamir and Adleman. It provides security by factorization and discrete logarithm intractability.

AES

Advanced Encryption Standard. It is a block cipher that encrypts 16-byte blocks using keys of length 128, 192 or 256 bits.

SHA1

Secure Hash Algorithm 1. The algorithm takes a message of a length of less than 264 bits and outputs a 160-bit message digest.

Key Generation

All implementations use a library to generate cryptographically secure random numbers following the guidelines in IETF RFC 1750 and pass tests from the NIST Special Publication 800-22, "A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications".

3.2.4 Tamper Resistance Techniques

Unlike cryptography, tamper resistance does not provide mathematically provably security; instead it increases the work factor for a specific attack. Each of the tamper resistant techniques defends against a specific attack, and they are applied together with other techniques to create layers of protection. In a software-only implementation, since the program code is executed on general purpose CPU's, the documented instruction set for the CPU must exist in clear-text in memory and thus it can be captured and analyzed. Tamper resistance protects against both static and dynamic analysis of the code as well as detects tampering such as code modifications.

Anti-Static Analysis

Static analysis is the use of tools to analyze the program code simply using the program files themselves. During static analysis the program is not actually executed, but is disassembled into a readable form and analyzed. Examples of anti-static analysis techniques include code encryption and operator expansion.

Anti-Dynamic Analysis

Dynamic analysis is the use of a debugger or processor emulation to trace the runtime execution of the program. Examples of anti-dynamic analysis include code segment signature checking, debugger detection and debugger disruption.

Key Hiding

Key hiding prevents the key for a cryptographic algorithm from completely existing in clear-text in memory at any time. The Helix DRM employs different key hiding techniques depending on the cryptographic algorithm and includes multiple techniques for each algorithm supported.

3.3 Security Architecture

3.3.1 Trusted Client

Two tamper resistance techniques are used in the Trusted Client, code segment signature checking, and Landmark Removal. Landmark Removal removes identifiable code patterns, strings, or constants from the code so a simple search for a well known pattern, string, or constant will not lead an attacker to an important piece of code to help them narrow their attack.

Renewability

Due to its pure software implementation and reliance on Tamper Resistance, the assumption is that the client will be hacked at some point in its lifecycle. To mitigate the effects of a successful attack, renewability is built into the system. When a component is compromised, it is revoked using best effort automated checking of Certificate Revocation Lists. Revocation can be done against content or components.

For PC platforms, the RealNetworks Auto Update technology is used to deliver an updated component to the client computer. The update is only as large as it needs to be to restore security, from as small as a single plug-in to as large as an entire new client.

For non-PC platforms, revocation will prevent consumption of the media until a field upgrade for the compromised component is made available.

3.3.2 Client Update Plug-in

Layers of tamper resistance protect the Client Update Plug-in. All operations on the Secure Database and media data are protected. Some of the tamper resistance techniques employed are: Code Encryption, Anti-debugging, Signature-Checking, Land Mark removal and Code Obfuscation.

3.3.3 Robustness Requirements

The Helix DRM implementations are built to the following requirements to ensure consistent, robust implementations.

- No backdoors: There must be no defeating functions that disable the security measures or rights enforcement, e.g. jumpers, configuration settings, keyboard combinations.
- Protect secrets keys and constants: All constants and secret keys must be protected from discovery in Tamper Resistant code. Use of techniques such as code encryption and key hiding must be used.

- Formal Robustness checks as part of Quality Assurance: These robustness requirements must be tested and accepted as operational as part of the Quality Assurance testing of every release of the product.

- Clear, compressed data not available on "user accessible" buses: A "user accessible" bus is defined as a data bus that is designed for end user upgrades or access, such as expansion card interfaces including PCMCIA, Compact Flash, Secure Digital Card, and PCI that has standard sockets or otherwise readily facilitates end user access. A "user accessible" bus does not include buses or portions internal device architecture that do not permit access to data in end user usable format such as the CPU memory bus or a co-processor bus.

- Distributed functions must be secured: If the implementation includes multiple independent processing units, such as a CPU and co-processor or dynamically loaded software libraries, they must authenticate and secure communications between the processing units.

- Self checking: The implementation must verify that program code has not been modified through a method such as check-sum or one way hash compared against a digitally signed production signature.

- Code encryption: If the device has a mechanism for accessing or updating the program code by end users, that program code must be encrypted.

- Privileged mode operation: If the implementation runs on an operating system that has multiple privilege levels, such as Kernel mode of Windows XP, portions of the implementation should be implemented to run at the highest privilege level.

- Code obfuscation: If the device has a mechanism for accessing or updating the program code by end users, that program code should be obfuscated.
- Self checking throughout operation: The implementation must perform self checking throughout operation, not only at initialization.
- Debugger detection: If the device has interfaces for debugging execution of program code, the implementation must detect the presence of a debugger and prevent its operation on the secure process.

3.3.4 License Storage

Licenses are stored in a secure database on the client machine, managed by the Client Update Plug-in. The database stores the rights for content and current state of those rights along with the encrypted content symmetric key and is indexed by the content ID. All operations on the secure database are performed within Tamper Resistant code.

3.3.5 Revocation

Revocation can be used to revoke rights for some content, revoke rights for all content from a given vendor and also to revoke certain compromised components in the client. Signature ID's are associated with each component in the system and these Ids can be revoked as needed.

3.3.6 Machine Binding

The Client Update Plug-in is bound to a machine. If the plug-in is installed on a machine that it is not bound to, it fails to operate. Likewise content licenses generated by the License Server are bound to a specific machine. This prevents licenses generated for one machine being loaded by another.

3.3.7 Trusted Packager

The Standard Helix DRM Packager is not protected by tamper resistant measures. As such, the distribution of the Packager is tightly controlled. Only Helix DRM licensees receive Packager software. The proposed system also allows for local packaging. When content is packaged locally all keys are handled with-in trusted modules utilizing the same tamper resistant techniques required for rights enforcement and playback.

Media Encryption

Media packets are encrypted with a symmetric key. The key is sufficiently strong that brute force attacks against the content take enough resources as to deter anyone from using brute force to crack multiple pieces of content. The packager will generate a new symmetric key for each file during packaging. It will alternately take a symmetric key to use as a parameter. All of the packets in a file will be encrypted. It is acceptable if for performance or other constraints the same algorithm or key cannot be used for every packet. If multiple algorithms/keys are used, the strongest algorithm/key is applied to the most critical data packets in the stream.

Algorithm Used: AES with a 128 bit key is used for encryption of media packets.

3.4 Supported Rights

Rights	Description	Default Value
Permanent Download Rights		
Allow Permanent Download	enables conversion of content to unsecure format	FALSE
Permanent Download Count	number of conversions allowed	Infinite
Playback Rights		
Allow Playback On PC	Enables playback on PC	TRUE
Duration From Download	calendar time after license is downloaded during which content can be played (seconds)	Infinite
Duration From First Play	calendar time after content is first played during which content can be played (seconds)	Infinite
Playback Count	Number of times content can be played	Infinite
Playback Threshold	playback time after which the playback count will be decremented (seconds)	30
Single Play Duration	(*Playback Count license only*) maximum time a single playback	1.5 * clip_length

Allow Secure Streamer	can run. **Must** be specified for live content. (seconds) Enables streaming to secure network connected device, i.e. DTCP / IP	FALSE

Transfer Rights

Allow Transfer To Non SDMI	enables transferring content to most devices, subject to other rights	FALSE
Allow Transfer To SDMI	enables transferring content to SDMI devices. **NOTE**: Currently there are no SDMI devices.	FALSE
Transfer Count	number of times content can be transferred	Infinite
Plays Per Transfer	number of plays on device for each transfer	Infinite
Required Device Capacity	required characteristics of device (see below)	None
Allow Transfer to BP	Enables transferring content to Broadcast Protected Content	FALSE

Device Characteristics

Field	Description	Current Options
DeviceID	identifier of the type of device	NetMD
DeviceName	name of the device	Sony NetMD

CD Rights

Allow Burn To CD	enables burning to CD	FALSE
Burn To CD Count	number of burns allowed	Infinite

Properties

License Duration	calendar time during which license will be valid (seconds)	None

Revocation Update Period	calendar time after which Revocation URL must be checked prior to playback (seconds)	None
Revocation URL	URL used for server-based revocation	None
Revoked Component	unique identifier for component which is being revoked	None
Allow Backup Restore	enables backup/restore feature	FALSE
Subscription GUID	unique ID of subscription under which license is also governed	None
Author	Author of licensed content	None
Copyright	Copyright of licensed content	None
Title	Title of licensed content	None

Actions

Revoke License	Revokes either a ContentGUID or SubscriptionGUID	None
Revocation Of Content	Revokes the vendor certificate, nullifying all content issued under that certificate	None

3.5 Transferring Secure Content to another Secure Device

With the growing market penetration of broadband and home networking within U.S. households, and with the future deployment of advanced devices supporting HDTV, Internet applications, and Broadcast Flag secured content, consumers will want to utilize these networks to deliver content within the home. Operators and content providers will want to deliver new services to consumers based on these capabilities.

To enable these new revenue models and consumer experiences, RealNetworks has designed Helix DRM from the start to be able to scale and grow into these markets. In

particular, the Helix DRM Trusted Recorder model, supporting Broadcast Flag, can be extended into other secure compliant devices in the home quite easily.

As one way to do this, RealNetworks has designed, released, and is currently shipping commercially the Helix Device DRM Protocol. The following outlines the functionality along with security and robustness requirements for the Helix Device DRM Protocol.

3.5.1 Abstract

This section specifies the Helix Device DRM key delivery protocol and associated robustness requirements. The protocol enables servers both as a part of a backend service or alternatively a PC or Set Top Box containing a Trusted Recorder ("Server") to act as an intermediary server to securely provision Helix Device DRM compliant keys with the appropriate Keys to consume or create content.

When content is packaged locally it is associated either with a default set of keys distributed with the Helix DRM Client.

3.5.2 Definitions

Content Key	Symmetric key used to encrypt a media file
Embedded License	Content Key encrypted with a User Key. The embedded License must also include the User ID.
Individually Licensed Content	Content requires an external license to manage its consumption.
Licensed User	User to whom a particular media file has been licensed.
User	A back end service account, consisting of, at a minimum,

	an User ID and User Key. A single account could have multiple User ID's that might represent a users different usage classes. IE, copy once content and copy never content. There must be a one to one mapping of a User ID to an associated User Key.
User ID	A 128 bit identifier linked to a Licensed User.
User Inaccessible Memory	A storage area on a device designed to store keys and other information. These areas should only accessible by software running on the Device and not readily readable and accessible from the PC.
User Key	Symmetric key linked to a User ID used to encrypt Content Keys
User Licensed Content	Content including an Embedded License and associated User ID linking content with a particular Licensed User. This content is bound to this user regardless of the device consuming that content.

3.5.3 Background

The Helix Device DRM protocol is designed to authorize devices to consume both User Licensed content and Individually licensed content.

User Licensed PC user experience

User licensed content is "personalized" or "bound" to a Licensed User at the time of content acquisition. The Content contains information about the User to whom the

content is licensed, and it also contains an encrypted Content Key required to decrypt the content during playback. The Content Provider assigns a unique User Key to each Licensed User. The User Key is used to encrypt the Content Key in every User Licensed content file. To consume the User Licensed content file, the User must register their PC, Set Top Box, or Consumer Electronics device with the Content Provider. Upon registration, the User will receive a License for a User ID that is appropriately associated with a User Key. This license will link in any associated Rights.

The License is kept in Secure Storage on the PC, Set Top Box, or CE device and is bound to the PC and to the User. Access to the User License enables access to User's class of content that is licensed under the associated User ID.

If the User wishes to use their content catalog on a different PC or device, they need to do two things: 1) copy their User Licensed content to the new machine, and 2) register the new PC with the Content Provider, thus obtaining a License with the User Key. The Content Provider may allow the User to play back their content on up-to "N" registered PCs or devices. This group of devices is often referred to as the concept of a user's "personal domain."

If the User has already registered "N" machines and attempts to playback their content on "N+1" machine, they will be asked to un-register one of their already registered machines before registering a new one. An un-registered machine removes the User's License disabling playback of User's content until the User chooses to re-license their machine.

For purposes of Broadcast Protection, each Flag State will be assigned a pre-defined User ID/User Key pair. When receiving BP Content, the packaging component will first encrypt the Content with a randomly generated symmetric key. Next, it will create an Embedded License using the User Key associated with the BP Flag detected in the source content. For those Flag States allowing copy (ie. Copy Freely, Copy Once), a transfer right will be enabled for that User ID license. For those Flag States not allowing copy (ie. Copy No More, Copy Never), no transfer right will be enabled.

Device User Experience

This protocol defines a secure method of allowing a Server to securely provision a device with a User Key. Once the device has been provisioned with a User Key, i.e. "registered" to the User, the device gains access to a User's entire library of content. The content can then be directly transferred from the Server to the device using any means available. The content is inert on its own and only becomes useful when a user transfers it to a registered device.

Under Broadcast Protection, the ability to transfer the User Key aligns with the Broadcast Protection Flag. If the User Key allows transfer, the Key will be copied. If the content requires modification during the copy process (e.g. changing from Copy Once to Copy No More), the source machine will rebind the content to the new User Key.

3.5.4 Protocol Overview

The Helix Device DRM protocol is designed to be easily adapted to devices with varying characteristics. The Server and device communicate via messages that can be passed asynchronously over any medium. This flexibility allows the messages to be passed

back and forth directly via device drivers or indirectly via drop boxes on dumb storage devices.

The Helix Device DRM protocol is broken into two stages:

a) Obtain Device Information (Device→Server)

b) Registration Message (Device←Server)

If the content is licensed on a local PC, then if the PC has the appropriate rights, the PC can act as a server and license content on a device. The server could also exist on an IP based network, and dynamically license the device directly, depending on the policy of the server.

The required behavior during these stages is generally the same across all devices.

See "Requirements for Message Processing" to see the device specific requirements. Devices are required to provide documentation explaining how they fulfill these requirements.

Obtain Device Information

The device must provide the device specific information to the Server in a standard format. The Server uses the device information to create individualized and confidential messages.

Dynamic and static Information must be transferred from the device to the Server. The dynamic information is generated on the device; it must be generated for each request.

The static data is contained in and referred to as the device certificate. The certificate is signed by RealNetworks and associated with highly confidential information embedded in trusted device code.

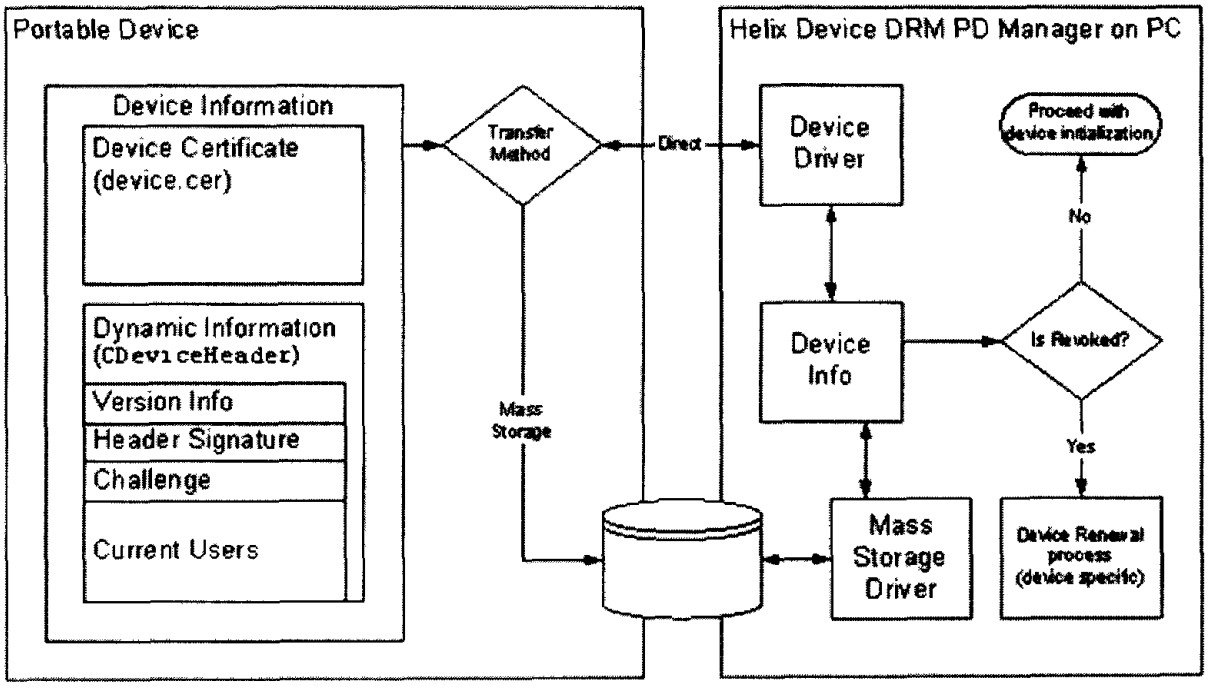


Figure 2 Device Information transfer to a Device DRM Server running on a PC

Dynamic Device Information

The dynamic device information must be generated on the device and updated after each message. The following requirements are on the Dynamic Device Info:

- The current users authorized to consume music on the device MUST be listed in the list of current users.

- The device ID is the unique device identifier. The unique device identifier is a constant and public identifier used to identify an individual device.
- The challenge is a unique number generated by the device. It should be initialized to be a random number, and it must not repeat to the same ID.
- A new signature with a fresh challenge should generally be created when the device is booted up. An exception would be when user inaccessible non-volatile memory is available to store the signature.
- The signature is signed/encrypted using the RSA private key or the device symmetric secret held by the device.

Device Certificate

The static device information is contained in the device certificate. RealNetworks provides a unique certificate embedded to embed in each player implementation. The certificate's format will be slightly different depending on whether the implementation is the asymmetric or symmetric protocol variant. The asymmetric certificate will contain the device's 1024 bit RSA public key for encryption. The symmetric certificates will contain the device's private symmetric key encrypted with a public RealNetworks RSA trusted key. The Server will utilize a trusted RealNetworks service to decrypt the device's private symmetric key.

The certificate is base64 encoded and generally should be treated as opaque data. The corresponding private or secret key MUST not be stored unprotected in user accessible memory. It must always be guarded with appropriate key hiding and tamper resistance techniques.

3.5.5 Registration Message

Once the Server has gained access to the device's information, the Server should have everything it needs to create a License and transfer a User key or content key to the device.

After the Server has retrieved the device information, it can create a registration message. This message is transferred to the device to register a specific the user or content ID on the device.

Upon receiving a message from the Server, the device must process and/or respond to the message.

Registration Process

When the PC wants to transfer content to a device it first retrieves the device information from the device.

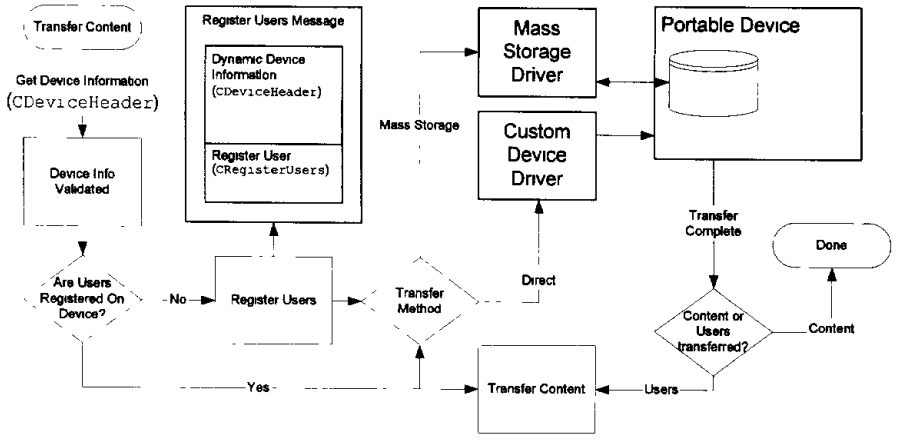


Figure 3 – Device Registration Process from PC

After verifying the certificate is valid, the PC ensures the user associated with the content is already on the device. If the user is on the device, the Server can transfer the content freely without updating the device.

If the user is not currently on the device, the Server checks to see if the user has rights to transfer to this device. If the user has sufficient rights an individualized registration message is created.

Registration Messages

In the symmetric case, an individualized device key is used to encrypt the CTransferKey structure. The encrypted device key is extracted from the certificate, then decrypted and individualized via communication with a private RealNetworks Service.

The registration message can be provisioned with multiple User Keys and Individual content Keys.

3.5.6 Individualization

The protocol can be implemented with asymmetric or symmetric cryptography. The asymmetric version of the protocol is designed for Devices that have an individualized private key. The downside of the asymmetric method is individualization can be a burden on manufacturing. Asymmetric cryptography can also be prohibitively expensive from a complexity point of view. The symmetric variant lessens this burden on device manufactures CPU. It also allows for individualization, but does not necessarily require every device be individualized with a confidential key. All devices must have a unique ID, but a certain number of devices could potentially share the same symmetric key.

3.5.7 Certificate Revocation

When the PC receives a certificate, it first must validate the certificate and check the certificate against its revocation list. It also checks the device ID against its revocation list. If the client is revoked, the PC issues a message to de-register all the users on the device.

3.5.8 Requirements for Message Processing

Helix Device DRM compliant device needs to appropriately implement several protocol related features for security reasons.

Device ID

Device ID in the message header is used by PC DRM to uniquely track each individual device. The device implementation should have a device ID that is not modifiable by the end user. A per device unique ID pre-embedded in the device ROM is the best

approach. The Device ID must be based upon at least one unique device hardware identifiers. If the Device ID is based on a combination of identifiers, the Device ID can be generated at an appropriate time (such as the first time device DRM runs) and saved to some non-volatile, non-user-accessible storage locations. Writable flash and a secret area on mass storage are two appropriate examples.

Challenge

The challenge value in the message header is used for replay attack prevention. It should be changed each time the device processes a new message in the body.

Protection for the message encryption key

In both symmetric and asymmetric version, the device needs to protect a secret device key (AES key or RSA private key). Adequate effort should be provided to hide these secret keys. Key hiding algorithm that blends the key into algorithm code is suggested to achieve this requirement. In no condition should these secrets keys be backed up in an unencrypted form to user-accessible storage or PC. The key should be held as highly confidential information and the robustness rules in "Robustness Requirements" should be followed.

Device internal key database

The device needs to maintain an internal database for user_id/content_id to user_key/content_key lookup. This internal database needs to be adequately protected since it contains user keys.

Device Certificate generation and handling

The reference code and documentation will initially come with a development keys and certificates. These keys should be used to create the device implementation and test it to insure that it follows the specification.

Each device implementation should embed a unique key. When production keys are needed the implementer will need to request keys from us.

3.5.9 Compliance Requirements

Applicability.

These rules are applicable to Licensed Products that have implemented playback functionality of Helix DRM Content.

Obligations regarding the persistent storage of content

Licensed products shall be constructed such that all Helix DRM Content is treated with care after decryption. Helix DRM content may not, once decrypted, be stored except for the sole purpose of enabling the immediate consumption of content but which (a) does not persist materially after the content has been consumed and (b) is not stored in a way which permits copying or storing of such data for other purposes.

3.5.10 Permitted outputs

Generally

As set forth in more detail below, a Licensed Product shall not pass Decrypted Helix DRM content, whether in digital or analog form, to an output except as permitted below.

Analog

There are no prohibitions relating to analog audio outputs.

Digital

Licensed Products shall not output Helix DRM Audio content in unprotected digital form.

Digital Output is allowed using approved output mechanism.

3.5.11 Robustness Requirements for Helix Device DRM

Overview

Participating clients shall be designed and manufactured so as to resist attempts to circumvent the functions of the specification as more specifically described below.

Defeating Functions and Features

Participating clients shall not include: (1) switches, buttons, jumpers or software equivalents, (2) traces that could be cut, or (3) features/functions (eg: service menus) which could be used to defeat any function of the specification.

The list of functions which cannot be thusly compromised includes but is not limited to:

1. Protection of the decrypted content
2. Protection of the RealNetworks provisioned Device Key or the RealNetworks Signed Individualized Private Key.
3. Enforcement of any associated playback restriction information.

Secrets Protection

Participating Clients shall be designed and manufactured such that they shall resist attempts to discover or reveal device keys or secret intermediate calculated cryptographic values.

3.5.12 Robustness requirements of software implementation

Any portion of a participating client that utilizes, in software, the RealNetworks Provisioned Device Key /RealNetworks Signed Individualized Private Key (Device Key)

and/or the decrypted User Key or content key should use any and all reasonable methods to frustrate efforts to obtain this key.

All software implementations must at a minimum include: (1) techniques of obfuscation to disguise, hamper and frustrate attempts to discover the approaches used to hide the use and value of the keys (2) self-checking of the integrity of its component parts and be designed to result in a failure to provide decryption in the event of unauthorized modification.

Further, they may include, but are not limited to: (1) code encryption (2) execution in kernel or supervisor mode (3) embodiment in a secure physical implementation that cannot be reasonably read.

3.5.13 Robustness requirements of hardware implementation

Any hardware component that utilizes the Device Key, or that relies upon hardware to satisfy these robustness rules shall: (1) embed Device Key and/or the decrypted User Key and content keys in silicon circuitry or firmware which cannot reasonably be read (2) be designed such that attempts to remove or replace hardware elements in a way that would compromise the RealNetworks Global Key/RealNetworks Signed Individualized Private Key and/or the decrypted User Key would pose a serious risk of damaging the Participating Device. By way of example, a component, which is soldered rather than socketed, may be appropriate for these means.

Hardware Data paths

Decrypted uncompressed data shall not be present on any user accessible buses in useable form. For this purpose user accessible bus is defined as: (1) an internal analogue connector which is designed for end user upgrades or readily facilitates end user access (2) a data bus that is designed for end user upgrades or access, eg: PCMCIA, CardBus, PCI bus.

A user accessible bus does not include memory buses, CPU buses or similar portions of a device's internal architecture.

3.5.14 Required Levels of Robustness

The levels of robustness described in sections throughout this section shall be implemented so that it is reasonably certain that, without physically disassembling the device, they cannot be defeated or circumvented using "Widely Available Tools" or "Specialized Tools", and that only with great difficulty they can be circumvented with "Professional Tools."

Widely Available Tools

Widely Available Tools is defined as general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips, file editors, and soldering irons.

Specialized Tools

Specialized Tools is defined as specialized electronic tools that are widely available at a reasonable price, such as memory readers and writers, debuggers, decompilers, or similar software development products.

Professional Tools

Professional Tools is defined as professional tools or equipment, such as logic analyzers, chip disassembly systems, or in circuit emulators.

4 Information Regarding Whether Content Owners, Broadcasters or Equipment Manufacturers Have Approved or Licensed the Digital Output Protection Technology Or Recording Method Affords Content

There are only two DRMs in the market that have currently been approved by both the major movie studios and major record labels for distribution of high-value content on the Internet: RealNetworks Helix DRM and Microsoft Windows Media DRM. Of these two, RealNetworks is the only company that licenses its DRM for use on any operating system.

Helix DRM is widely used and adopted in the commercial marketplace. There are over 500,000 songs encrypted and secured using Helix DRM through a combination of the MusicNet and Rhapsody services. There are over 700 movie titles currently offered by the Movielink service that are encrypted and secured using Helix DRM.

Content owners and services who have approved the use of Helix DRM for distribution of their content on the Internet include:

- Movielink
- Metro Goldwyn Mayer
- Paramount
- Warner Brothers
- Universal
- Sony Pictures
- Triggerstreet.com

- MusicNet
- Universal Music
- Zomba
- Sony Music
- EMI
- BMG
- Warner Brothers Music
- Starz Encore Group

Other publicly announced companies using Helix DRM include:

- BBC
- BT Broadcast Services CandW
- Creative Labs (Helix Device DRM)
- DTAG (Deutsche Telecom)
- DTAG-2
- Entriq
- NTL
- NTT-Cyber
- palmOne (Helix Device DRM)
- PortalPlayer (Helix Device DRM)
- Telecom Italia
- Tiscali
- T-Systems
- TTNet

- ViaAccess

Other companies have licensed and use Helix DRM to deliver secure content but are confidential and thus not listed here.

As an example of a commercial service using Helix DRM in the marketplace, a screenshot of the Movielink service is included below. The example shows that the downloaded media is secure and in this business use case, indicates to the consumer that the rights associated with the content expire in 24 hours.

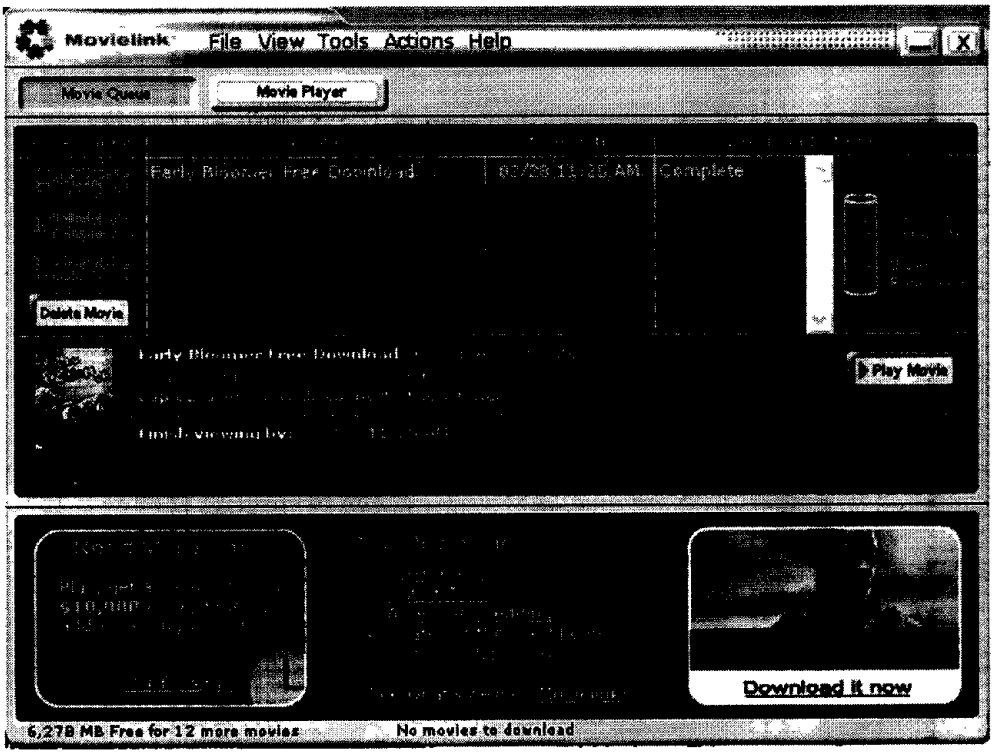


Figure 4. Screenshot of Movielink commercial VOD service using Helix DRM

As an example of a consumer electronics device supporting the Helix Device DRM protocol, a screenshot of the RealPlayer for Palm is included below. The Helix Device DRM protocol ships with seven palmOne devices, including the Treo 600, Zire 71, Tungsten T, C, E, T2, T3. Usage of the Helix Device DRM protocol is seamless to consumers and there are no adverse consumer experiences.

Figure 5. Screenshot of the commercially available RealPlayer for Palm, using the Helix Device DRM protocol.

5 If the Technology is to be Offered Publicly, a Copy of its Licensing Terms and Fees, as well as Evidence Demonstrating that the Technology Will Be Licensed on a Reasonable, Non-Discriminatory Basis

RealNetworks licenses Helix DRM for use on any operating system and with any device. We make our technology widely available and our pricing is designed to encourage high volume adoption and ubiquity of deployment.

The proposed technologies enabling Helix DRM to support Broadcast Flag in this certification request document, if certified, will be made available publicly on a reasonable, non-discriminatory basis, falling in-line with current business practices. Our market objectives are to drive penetration and widespread adoption of Helix DRM Trusted Recorder and Helix Device DRM into consumer devices. We will thus follow the RAND path established by the successful RAND based licensing program RealNetworks has established in the Helix Community initiative.

The Helix Community shows how RealNetworks makes its technology available on a RAND basis: the widespread licensing of the Helix DNA Client, which is the foundation and necessary client technology on which the Helix DRM Trusted Recorder is based, has taken place because of its RAND-based licensing program. As a part of this program, RealNetworks has posted its standard Helix licenses, available publicly, at www.helixcommunity.org. In addition, over 5,000 companies and individuals have already licensed the Helix DNA Client including many consumer electronics manufacturers and suppliers including (but not limited to) as ACCESS, ATI, BSQUARE, CAC Media, Equator Technologies, Ericcson, Hitachi, IBM, Intel, Lafayette Electronics,

Motorola, NEC, palmOne, PortalPlayer, Prismiq, Renesas, Rockford Corporation, Sharp Corporation, Sigma Designs, Simple Devices, Sony, STMicroelectronics, Sun Microsystems, Texas Instruments, Toshiba. The widespread licensing of the Helix DNA Client is significant because it means device manufacturers recognize and support the RAND based program, and provides a solid foundation for the addition of Helix DRM Trusted Recorder technology to the Helix Community.

APPENDIX

Appendix: RealNetworks Company Overview

RealNetworks is the leading provider of Internet protocol (IP) network delivered digital audio and video services and the creator of the technology that enables digital media creation, distribution and consumption. Consumers use RealNetworks Real Player 10 and RealNetworks content subscription service, RealOne SuperPass, to play free and premium digital audio and video content in an interactive manner. Broadcasters, network operators, media companies and enterprises use RealNetworks products and services to deliver digital media to PCs, mobile phones and consumer electronics devices.

Universal. In 2002 RealNetworks released the first truly universal media delivery software platform. For example, the Helix Universal Server product line supports streaming RealAudio, RealVideo, MP3, Windows Media, QuickTime, MPEG-4 and approximately 50 other media formats.

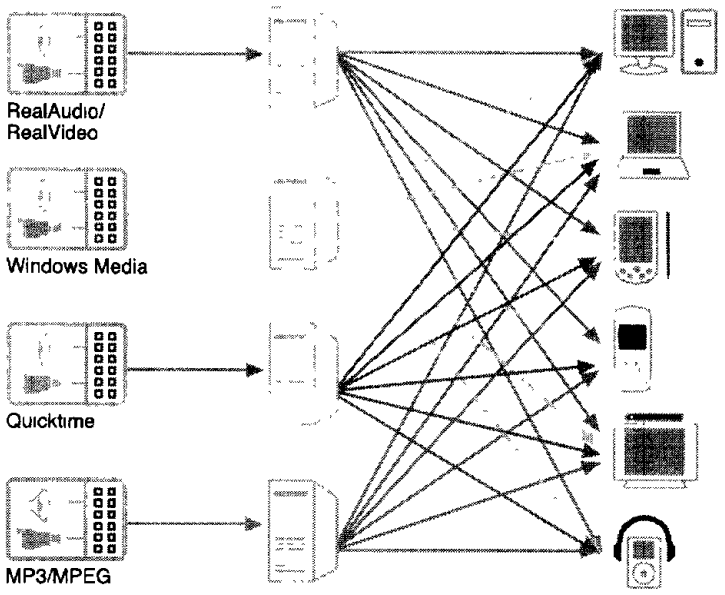


Figure 6. IP Delivered Media Landscape Before Helix

The benefits to network and hosting providers were clear – no more need to maintain multiple infrastructures. Similarly, the Real Player 10 Plus discovers, manages and plays content in each of the major Internet and standards based media formats – providing the consumer a single desktop application for all digital media. Finally, Helix DRM provides the first, and only, software solution for the secure delivery of standards-based formats as well as leading Internet formats for streaming or downloading.

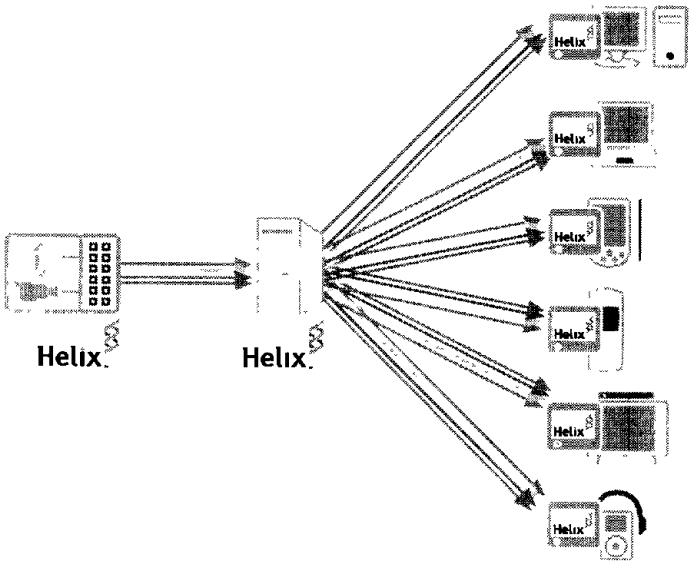


Figure 7. IP Media Delivery Landscape with Helix

Standards. RealNetworks has always contributed to industry standards and supported them in products. For example, RealNetworks co-authored and led the standardization effort in IETF for Real Time Streaming Protocol (RTSP). Similarly, RealNetworks was a co-contributor to the specification development for SMIL or the Synchronized Multimedia Integration Language – an XML based language to create rich media presentations. RealNetworks was the first to implement both standards in commercially shipping products and continues to support both. Additionally, RealNetworks continues to contribute actively to a number of current and ongoing standards including MPEG4, H.264 as well as the Open Mobile Alliance (OMA).

Open. RealNetworks launched the Helix Community in response to the increased breadth of emerging non-personal computer devices with digital media or IP delivered media capabilities. For example, RealNetworks is working with Nokia and others in the mobile phone industry through the Helix Community to create media players for those

devices that support standards based formats and protocols as well as common Internet formats and protocols. Key portions of RealNetworks 9th generation system and player software source code have been made available at HelixCommunity.org under both a reasonable and non discriminatory commercial license as well as under an OSI certified community license. Both licenses are 'click to accept' and allow research and development to occur without any up-front investment from the licensee. The Helix DNA Client, the foundational technology for Helix DRM, has been ported or is actively being ported to the wide range of operating systems, including all of the most popular operating systems used by the Consumer Electronics industry: Linux, WinCE, iTron, PSOS, VXWorks, Palm, Symbian, SmartPhone, MAC, Windows.

RealNetworks uses its own products and services to create and manage the media subscription services that are distributed directly to consumers as well as through distribution partners. RealOne SuperPass is a premium media service with selected content from news, entertainment, radio as well as sports leagues and other webcasters. RealOne Arcade is a PC game application that helps consumers discover, manage and purchase downloadable games. RealOne RadioPass is a premium music subscription service. In August 2003, RealNetworks closed the purchase of Listen.com, the developer and provider of the best in class music subscription service called RHAPSODY. RealNetworks also is founder and remains a technology partner of the MusicNet music subscription service offered currently by AOL/Time Warner.

Rob Glaser, the current chairman and CEO, founded RealNetworks in 1994. The first RealPlayer was released in 1995. Today, more than 335 Million unique users have

been registered. Since the early days, RealNetworks has been focused on delivering digital media to consumers over narrowband and, increasingly, broadband networks.

-end-